CLAIMS

1. A method for configuration management for a computing device, comprising the steps of:

providing available software to said computing device through an interface;

determining whether or not resident software stored in a storage device associated with said computing device is authenticated; and

loading said available software into said storage device if said resident software has not been authenticated.

2. The method of claim 1 further comprising the steps of:

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

loading said available software if said resident software is authenticated and said available software is authenticated.

3. The method of claim 1 wherein the step of determining whether or not said resident software is authenticated comprises the steps of:

determining whether or not an authentication flag has been set;

wherein said resident software is determined to be authenticated if said authentication flag has been set; otherwise

said resident software is determined to be unauthenticated.

4. The method of claim 3 wherein said authentication flag is set when authenticated software has been loaded onto said computing device.

5. The method of claim 3 wherein said authentication flag is set by a service technician.

6. The method of claim 1 wherein the step of determining whether or not said resident software is authenticated comprises the step of performing a direct authentication procedure on said resident software.

7. The method of claim 6 wherein said direct authentication procedure comprises performing a cyclic redundancy check.

8. The method of claim 6 wherein said direct authentication procedure comprises performing a secure hashing algorithm.

9. An apparatus for performing configuration management for a computing device, comprising:

an interface for providing available software to said computing device;

a storage device for storing resident software and a set of executable computer instructions for determining whether or not said resident software is authenticated;

a processor for executing said set of executable computer instructions and for loading said available software if said resident software is authenticated.

10. The apparatus of claim 9 wherein:

said set of executable computer instructions is further for determining whether of not said available software is authenticated;

said processor is further for rejecting said available software if said resident software has been authenticated and said available software is not authenticated; and

said processor is further for loading said available software if said resident software is authenticated and said available software is authenticated.

11. The apparatus of claim 9 wherein:

said storage device is further for storing an authentication flag for indicating the authentication status of said computing device; and

said processor is further for determining whether or not said resident software is authenticated based on said authentication flag.

12. The apparatus of claim 11 wherein said authentication flag is set when authenticated software is loaded onto said computing device.

13. The apparatus of claim 11 wherein said authentication flag is set by a service technician.

14. The apparatus of claim 9 wherein said processor is further for performing a direct authentication procedure on said resident software to determine whether or not said resident software is authenticated.

15. The apparatus of claim 14 wherein said direct authentication procedure comprises performing a cyclic redundancy check.

16. The apparatus of claim 14 wherein said direct authentication procedure comprises performing a secure hashing algorithm.